CLAIMS

1. (Presently amended) An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the intrusion detection system comprising:

means for monitoring activity relative to said computer system or network;

means for receiving and storing one or more general rules, each of said general rules being representative of the effect on the computer system or network arising from a plurality of specific instances of intrusion or attempted intrusion; and

matching means for receiving data relating to activity relative to said computer system or network from said monitoring means and for comparing, in a semantic manner and independently of the syntax of the activity, sets of actions forming said activity against said one or more general rules to identify an intrusion or attempted intrusion.

2. (Previously presented) An intrusion detection system according to claim 1, wherein said one or more general rules forms a knowledge base of the system, and wherein the system comprises means for automatically generating and storing in said knowledge base a new general rule representative of the effect on the computer system or network arising from specific instances of intrusion or attempted intrusion not previously taken into account.

3. (Original) An intrusion detection system according to claim 2, wherein said means for automatically generating and storing a new general rule comprises inductive logic programming means.

4. (Previously presented) An intrusion detection system according to claim 3, wherein said one or more general rules is or are represented in a logic programming language.

5. (Previously presented) An intrusion detection system according to claim 3, wherein inductive logic programming techniques are applied by the system to an attack, an intrusion, or attempted intrusion.

6. (Presently amended) An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the intrusion detection system comprising:

means for monitoring activity relative to said computer system or network;

means for initially receiving and storing a knowledge base comprising one or more general rules, each of said general rules being representative of the effect on the computer system or network arising from a plurality of specific instances of intrusion or attempted intrusion and being independent of the syntax of the activity; and

means for automatically generating and storing in said knowledge base (after said knowledge base has been initially stored) new general rules representative of the effect on the computer system or network arising from specific instances of intrusion or attempted intrusion not previously taken into account.

7. (Presently amended) An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the intrusion detection system comprising:

means for monitoring activity relative to said computer system or network;

means for initially receiving and storing in a knowledge base data representative of the effect on the computer system or network arising from one or more specific instances or classes of intrusion or attempted intrusion;

matching means for receiving data relating to activity relative to said computer system or network from said monitoring means and for comparing in a semantic manner and independently of the syntax of the activity, sets of actions forming said activity against said stored data to identify an intrusion or attempted intrusion; and

inductive logic programming means for updating said stored data to take into account the effect on the computer system or network arising from further instances or classes of intrusion or attempted intrusion occurring after said knowledge base has been initially received and stored.

8. (Canceled)

9. (Previously presented) An intrusion detection system according to claim 1, wherein said one or more general rules is or are represented in a logic programming language.

10. (Previously presented) An intrusion detection system according to claim 2, wherein said one or more general rules is or are represented in a logic programming language.